МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы построения защищенных компьютерных сетей

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью изучения дисциплины «Основы построение защищенных компьютерных сетей» является теоретическая и практическая подготовка обучающихся к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях. Задачи дисциплины: - изучение типовых угроз безопасности в компьютерных сетях; - изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях; - приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях; - овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем; - овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-10 - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

ОПК-17 - Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма;

ПК-7 - Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации;

ПК-9 - Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию;

ПК-11 - Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации;

ПК-12 - Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Уметь:

Выполняет задачи по администрированию подсистем и средств защиты информации в КС.

Уметь:

Выполняет задачи по администрированию подсистем и средств защиты информации в сетях.

Уметь:

Владеет методами и средствами оценки эффективности операционных систем и систем управления базами данных.

Уметь:

Умеет применять на практике методы и средства оценки эффективности операционных систем и систем управления базами данных.

Уметь:

Умеет проводить дифференциацию и декомпозицию задач оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных.

Уметь:

Умеет анализировать результаты оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.

Владеть:

Владеет методами и средствами контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях.

Уметь:

Умеет применять на практике методы и средства контроля корректности функционирования программно-аппаратных средств защиты информации в

компьютерных системах и сетях.

Уметь:

Умеет проводить дифференциацию и декомпозицию задач контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях.

Уметь:

Умеет анализировать результаты контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.

Уметь:

Проводит анализ безопасности компьютерных систем, в том числе с использованием методов моделирования, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.

Уметь:

Участвует в проведении экспериментально- исследовательских работ при аттестации объектов с учетом требовании? к уровню защищенности компьютерной системы.

Уметь:

Вырабатывает рекомендации в связи с проведенным анализом безопасности, в том числе для принятия решения о повторной аттестации компьютерной системы (в том числе автоматизированных систем), предложения по устранению выявленных уязвимостей.

Уметь:

Обосновывает критерии и рассчитывает показатели эффективности защиты обрабатываемой информации.

Уметь:

Составляет методики тестирования, подбирает инструментарии? и осуществляет проверку эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации.

Уметь:

Выполняет работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.

Уметь:

Выполняет работы, связанные с реализацией частных политик информационной безопасности автоматизированной системы.

Уметь:

Проводит мониторинг и аудит безопасности компьютерной системы в сфере профессиональной деятельности.

Уметь:

Формирует основные показатели и критерии эффективности, оценивает эффективность компьютерной системы и ее средств защиты в области профессиональной деятельности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Сем. №8
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 80 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован

полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	КС и их организация / Сетевые атаки.
2	Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI
3	Механизмы реализации атак в сетях TCP/IP./
4	Методы сканирования портов. Методы обнаружения пакетных снифферов. Методы обхода МЭ.
5	Методы перехвата сетевых соединений в сетях TCP/IP./
6	Технические меры защиты от сетевых атак. Атаки направленные на сетевую инфраструктуру
7	Примеры сетевых атак в сетях TCP/IP.
8	Технические меры защиты от сетевых атак
9	Принуждение к ускоренной передаче..
10	Атаки,направленные на отказ в обслуживании.
11	Изменение конфигурации и состояния хостов. Программно-технические меры защиты от сетевых атак
12	Криптографические методы защиты информации в компьютерных сетях.
13	Криптографические протоколы обеспечения безопасности.
14	Протоколы аутентификации на прикладном уровне. Протокол Kepberos.
15	Протоколы аутентификации на транспортном уровне: протокол SSI/TLS/
16	Защита виртуальных частных сетей (VPN).
17	Назначение, основные возможности и варианты реализации VPN.
18	Достоинства и недостатки применения VPN
19	Протокол IPSEC/ Протоколы AH и ESP.
20	Использование протокола L2TP для организации виртуальных частных сетей.
21	Разработка защищенных сетевых приложений.
22	Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI.
23	Программный интерфейс Open SSI.

№ п/п	Тематика лекционных занятий / краткое содержание
24	Программно-аппаратные средства обеспечения безопасности в компьютерных сетях.
25	Средства защиты локальных сетей при подключении к Интернет.
26	Место и роль МЭ в обеспечении сетевой безопасности. Основные возможности и схемы развертывания МЭ
27	Методы сетевой трансляции адресов (NAT).
28	Построение правил фильтрации. Реализация сетевой политики безопасности с использованием МЭ.
29	Методы обхода межсетевых экранов
30	Защита серверов и рабочих станций.
31	Системы обнаружения вторжений (СОВ). Место и роль СОВ в общей системе обеспечения сетевой безопасности. Классификация СОВ.
32	Средства и методы предотвращения в обнаружении вторжений.
33	Выявление атак на основе сигнатур атак и выявление аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Системы виртуальных ловушек (Honey Pot и Paded Geet).

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ 1 Инструментальные средства проведения атак
2	ПЗ 2 Методы и средства перехвата в сетях TSP/IP
3	ПЗ 3 Технические меры защиты от сетевых атак
4	ПЗ 4 Развертывание VPN с использованием IPSEC
5	ПЗ 5 Обеспечение целостного с использованием программного интерфейса SSPI
6	ПЗ 6 Развертывание VPN базовыми средствами ОС Linux с использованием L2TP.
7	ПЗ 7 Настройка и использование встроенного пакетного фильтра ОС Linux iptables.
8	ПЗ 8 Настройка и использование прокси-сервера SQUID
9	ПЗ 9 Использование и настройка средства обнаружения вторжений Snort

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР 1 Основные виды угроз для протоколов TCP/IP и OSI
2	СР 2 Методы сканирования портов
3	СР 3 Технические меры защиты от сетевых атак.
4	СР 4 Принуждение к ускоренной передаче
5	СР 5 Современные средства в компьютерных сетях
6	СР 5 Современные средства в компьютерных сетях
7	СР 5 Современные средства в компьютерных сетях
8	СР 6 Протоколы, обеспечивающую работу VPN
9	СР 6 Протоколы, обеспечивающую работу VPN
10	СР 6 Протоколы, обеспечивающую работу VPN
11	СР 7 Проблемы и реализация защиты сетевых приложений
12	СР 8 Проблемы и реализация защиты сетевых приложений
13	СР 9 Методы обхода межсетевых экранов
14	Выполнение курсовой работы.
15	Подготовка к промежуточной аттестации.
16	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1) Технология SIEM и ее функциональные возможности. Преимущества и недостатки по сравнению с другими решениями. 2) Сетевые пакетные фильтры и их разновидности. 3) Посредники и особенности их применения для сетевой защиты. 4) Технология NAT и варианты ее развития 5) Сеансовый посредник SoC и специфика его применения 6) Инспекторы состояния как инструмент фильтрации для обеспечения требуемого уровня ИБ. 7) Обеспечение межсетевой защиты ресурсов посредством UTM-устройств и NG firmware 8) Виртуальные частные сети и наиболее часто используемые протоколы VPN 9) Характеристика и архитектура протокола IPsec. 10) Системы обнаружения вторжений структуры и принципы построения 11) Сравнительный анализ систем обнаружения вторжений и для сетевой

безопасности 12) DLP-системы и их возможности. Анализ часто применяемых DLP-систем. 13) Сетевые сканеры уязвимостей, как средства анализа защищенности сетей 14) Ловушки, как средство сбора информации о злоумышленнике. 15) Защита локальных вычислительных сетей от атак канального уровня 16) Защита информации от ПЭМИН 17) Обеспечение аутентификации пользователей и разграничение доступа к информационным ресурсам 18) Обеспечение защиты информационных ресурсов компании от сетевых атак 19) Построение систем безопасности сетевого уровня на базе протокола IPSec 20) Построение отказоустойчивой ЛВС на базе протокола STP 21) Защита рабочих станций сети от вредоносного ПО и несанкционированных действий сотрудников 22) Защита информации и конфиденциальных данных, передаваемых по e-mail 23) Система обнаружения вторжений RealSecure 24) Управление ключами в вычислительных системах 25) Инструментальные средства предотвращения сетевых атак

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта В.В. Яковлев, А.А. Корниенко Однотомное издание УМК МПС России , 2002	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
2	Компьютерные сети. Принципы, технологии, протоколы В.Г. Олифер, Н.А. Олифер Питер , 2006	НТБ (уч.3)
1	Стандарты ИБ. Курс лекций Галатенко В.А. ИНТУИТ.РУ, Интернет-Университет Информ. Технологий М. ,	
2	Безопасность корпоративных сетей Биячуев Т.А. СПБ , 2006	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Корниенко А.А. , Слюсаренко И.М., 2009 на сайте FORUM

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Требования к программному обеспечению и перечень информационных технологий используемых при прохождении учебной дисциплины1.

распространяемая система виртуализации Virtual Box. 2. Операционная система Linux. 3. Свободно распространяемый пакетный фильтр iptables. 4. Свободно распространяемый прокси-сервер SQUID. 5. Свободно распространяемые ПО для организации виртуальных сетей OPEN VPN. 6. Свободно распространяемая система обнаружения вторжений Snort. 7. Свободно распространяемый сервер удаленного доступа OPENSSH.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Должно быть предусмотрено наличие компьютерного класса и интерактивная доска.Для практических занятий необходимоналичие компьютерного класса, объединенного в локальную вычислительную сеть. На компьютерах должны быть установлены серверные версии ОС Linux (или ОС в рамках виртуальных машин). В качестве коммуникационного оборудования могут использоваться коммутаторы, позволяющие организовать VLAN. Желательно доступ в Интернет. Желательно, чтобы студенты имели при себе носители информации (flash-накопители).

9. Форма промежуточной аттестации:

Курсовая работа в 8 семестре.
Экзамен в 8 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы

Профессор, профессор, д.н. кафедры «Управление и защита информации»	Клепцов Михаил Яковлевич

Лист согласования

Заведующий кафедрой УиЗИ	Л.А. Баранов
Председатель учебно-методической комиссии	С.В. Володин